МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

Лабораторная работа №1

ОТЧЕТ

по лабораторной работе

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В. Е.

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Прядилов А. С.

(подпись) (фамилия, и.,о.)

19-АС

(шифр группы)

Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2022

**Задание на работу:**

**Работа с анализатором протоколов tcpdump**

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов возпользоваться утилитой ping.

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

**Работа с анализатором протоколов wireshark**

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

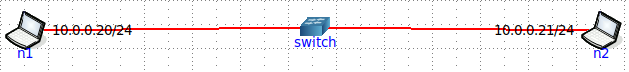
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

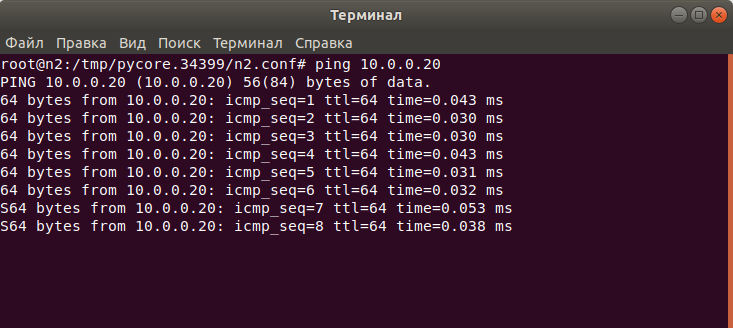
4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

**Задание 1:** запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

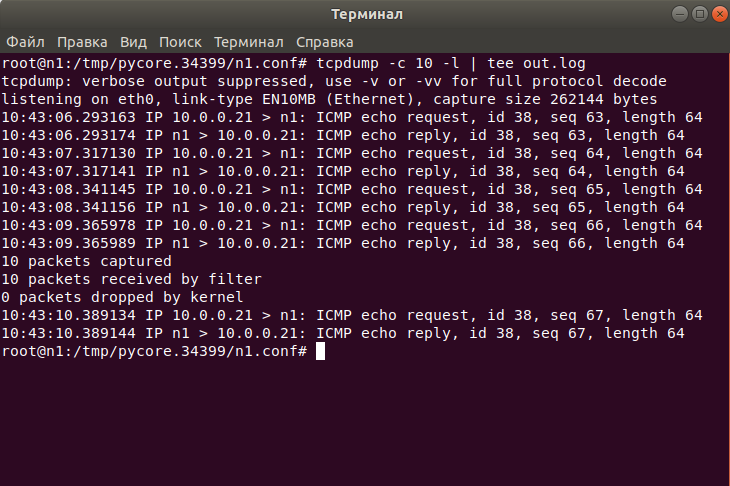
Структура сети:

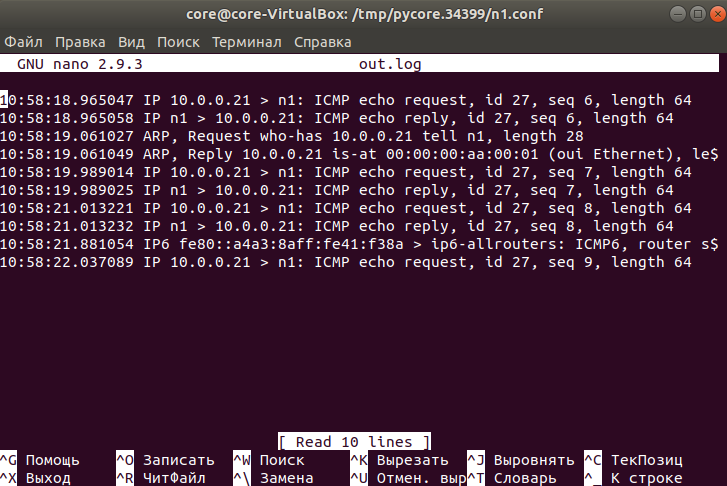


Начинаем передачу пакетов с компьютера PC2 на PC1:

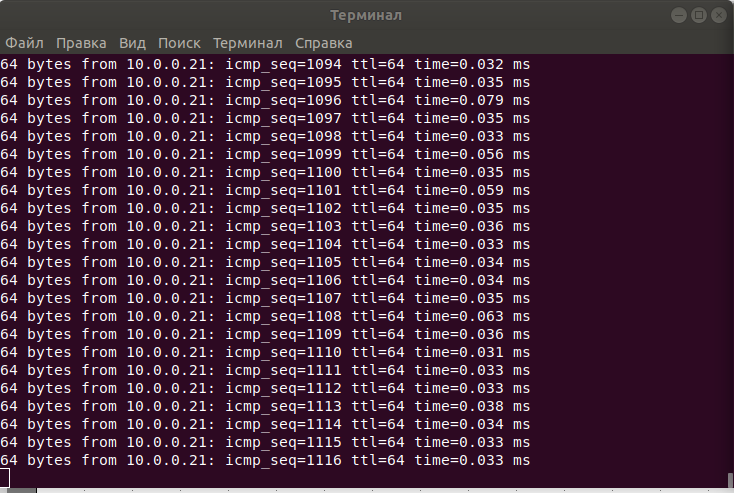


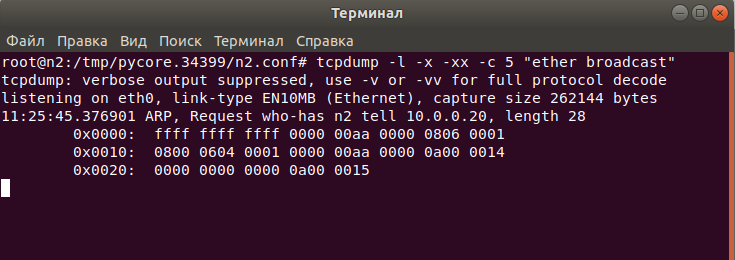
На PC1 запускаю **tcpdump** с необходимыми параметрами:





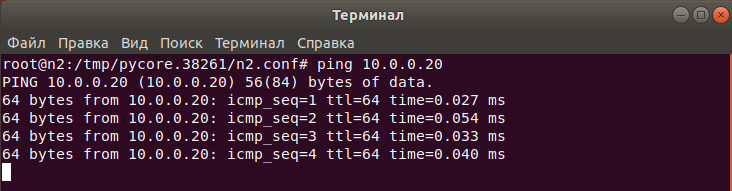
**Задание 2:** запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).



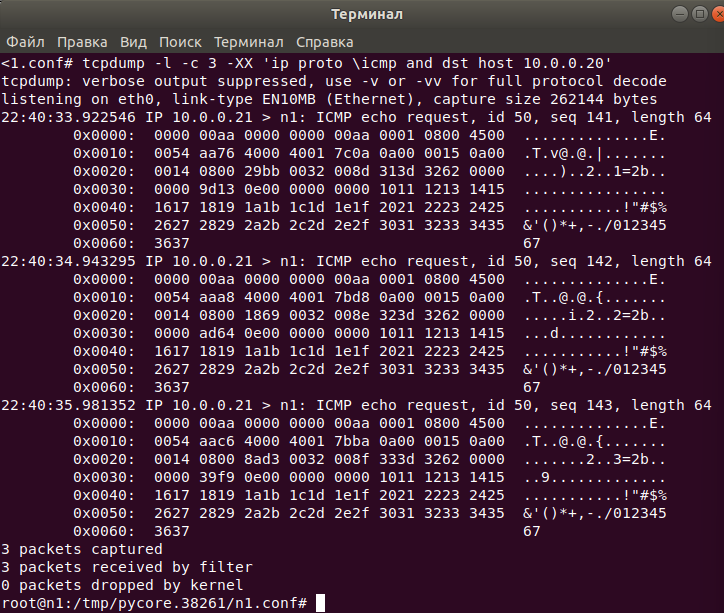


**Задание 3**: запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

Снова начнём с передачи пакетов с компьютера PC2 на PC1:

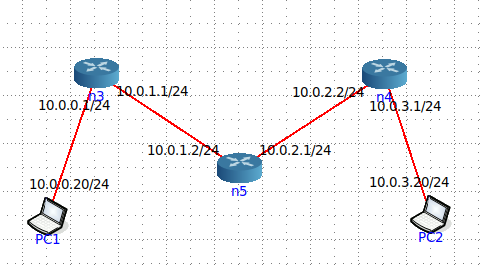


Параллельно с этим запускаем tcpdump на 1-ом компьютере и пропишем вместе с ним нужные параметры и фильтры, которые помогут перехватывать только пакеты ICMP.

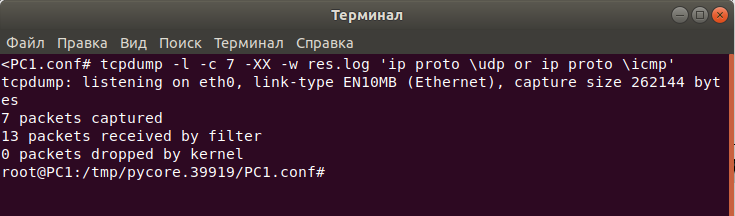


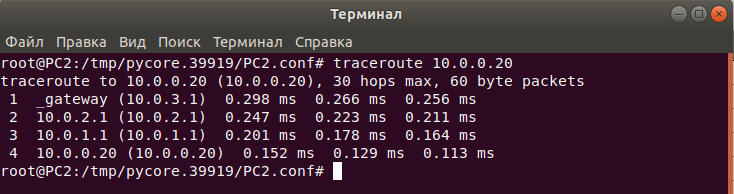
**Задание 4:** запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.

Соберу сеть:

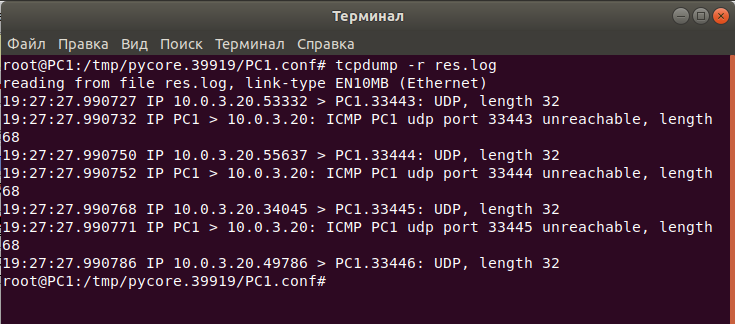


Запустим tcpdump на PC1 с нужными параметрами, фильтрами и одновременно передадим пакеты с компьютера PC2 с помощью утилиты traceroute:



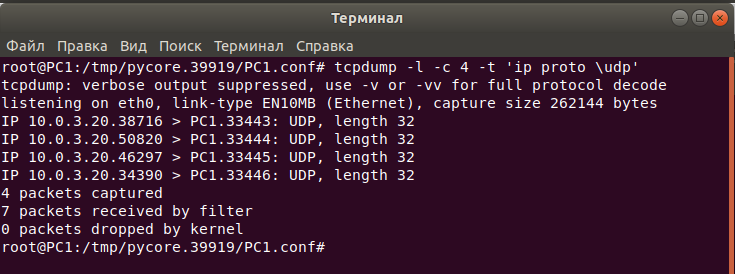


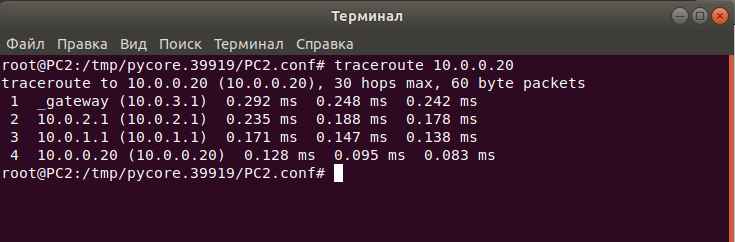
**Задание 5:** прочесть программой tcpdump созданный в предыдущем пункте файл.



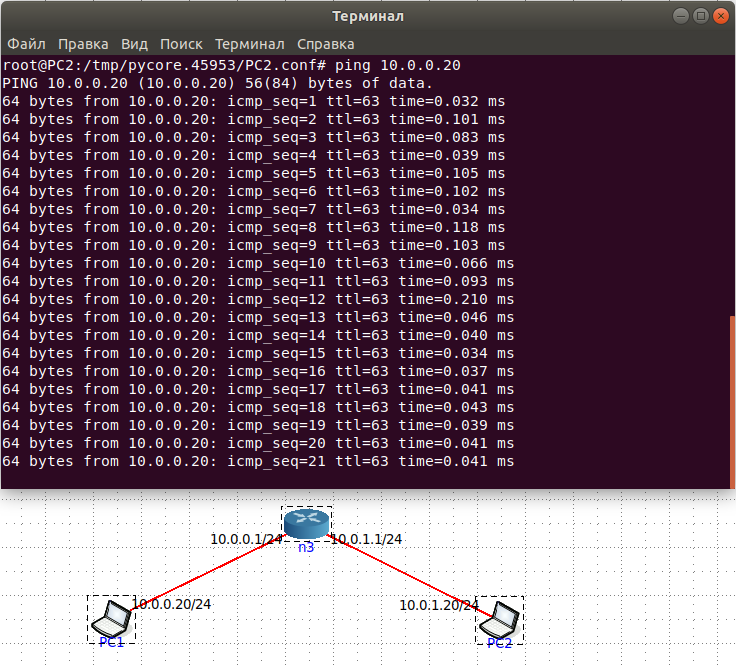
**Задание 6**: придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

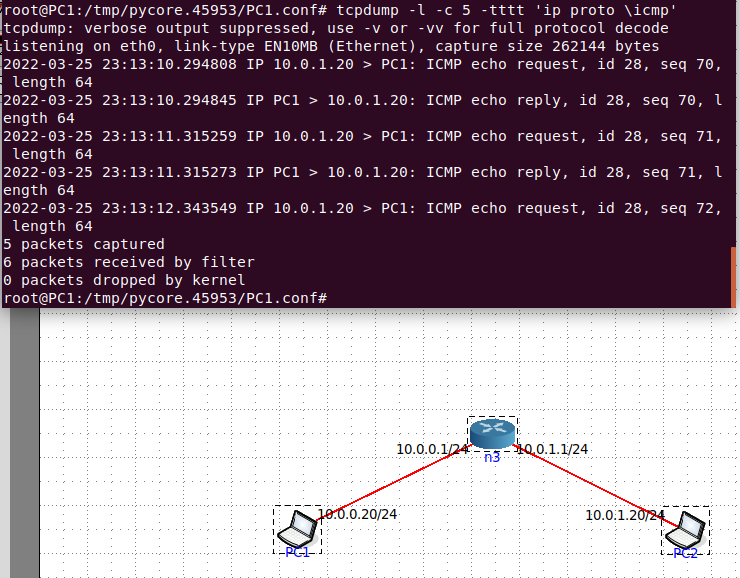
1) Запустить tcpdump, перехватывающий пакеты с фильтром протокола UDP. Не отображать метку времени в каждой строке. Количество захватываемых пакетов ограничить до 4. Для передачи пакетов воспользоваться утилитой traceroute.



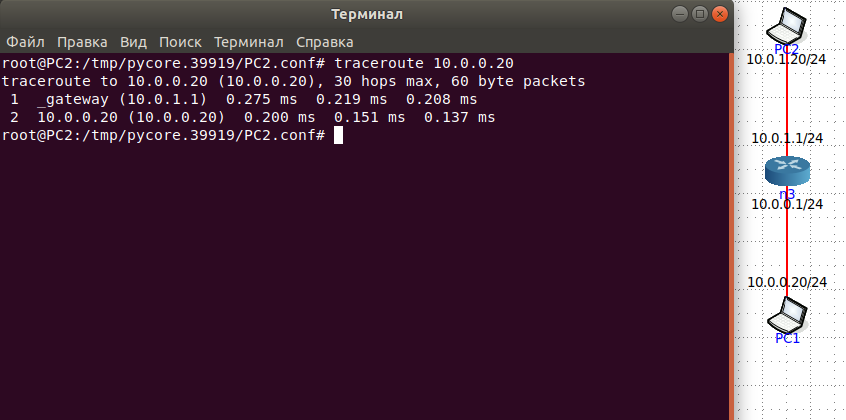


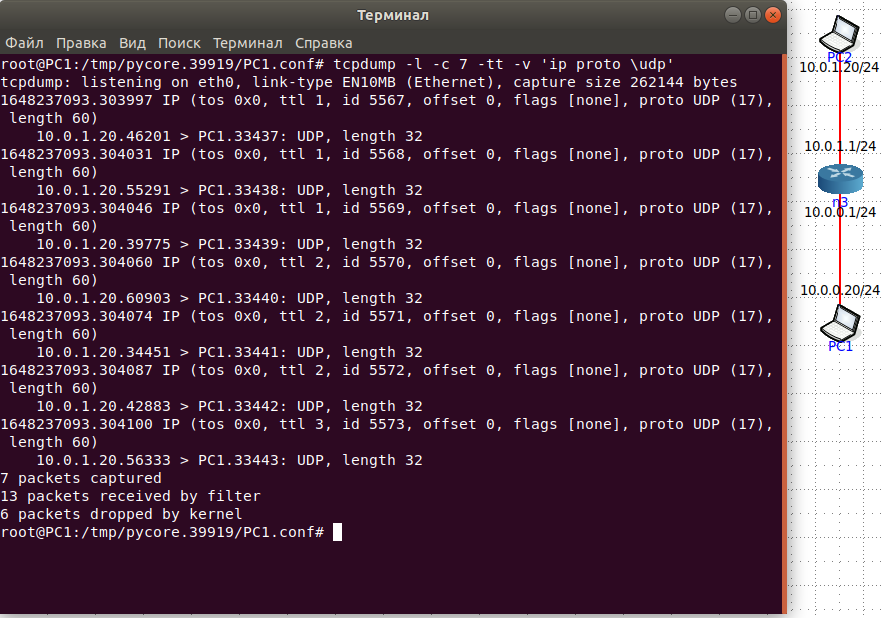
2) Запустить tcpdump, перехватывающий пакеты с фильтром протокола ICMP. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 5. Показать дату и время.





3) Запустить tcpdump, перехватывающий пакеты с фильтром протокола UDP. Отобразить время. Количество захватываемых пакетов ограничить до 7. Вывести подробную информацию. Для передачи пакетов воспользоваться утилитой traceroute.

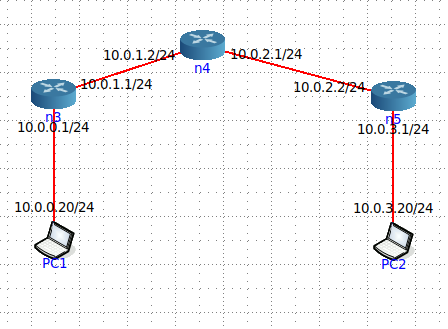


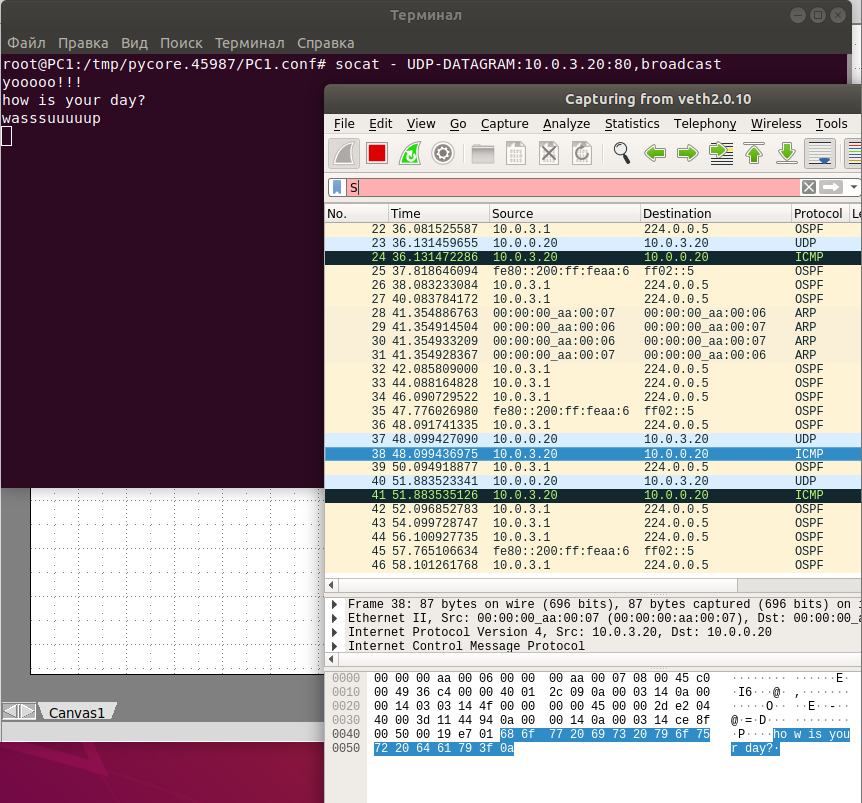


Работа с анализатором протоколов Wireshark

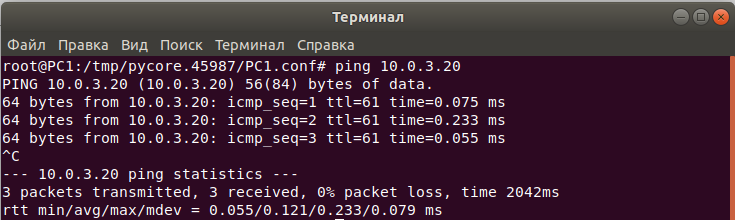
1) Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

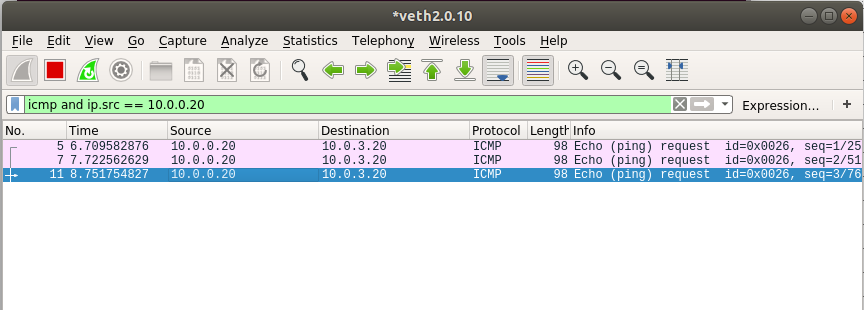
Структура сети:





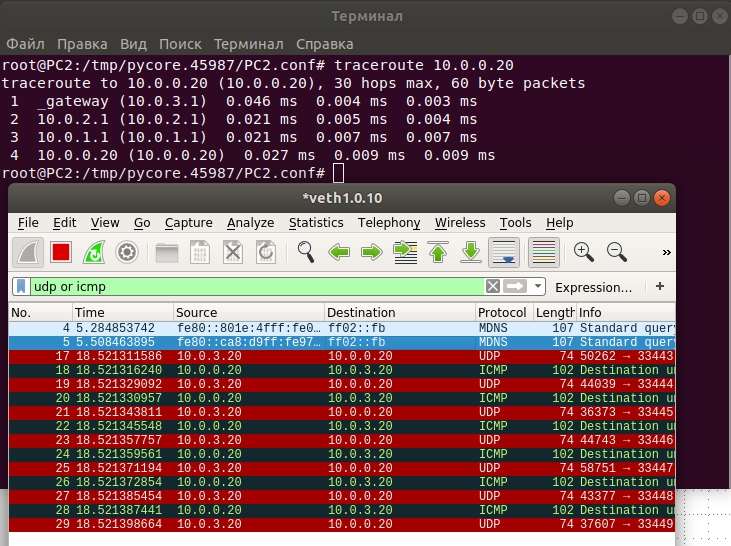
2) Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



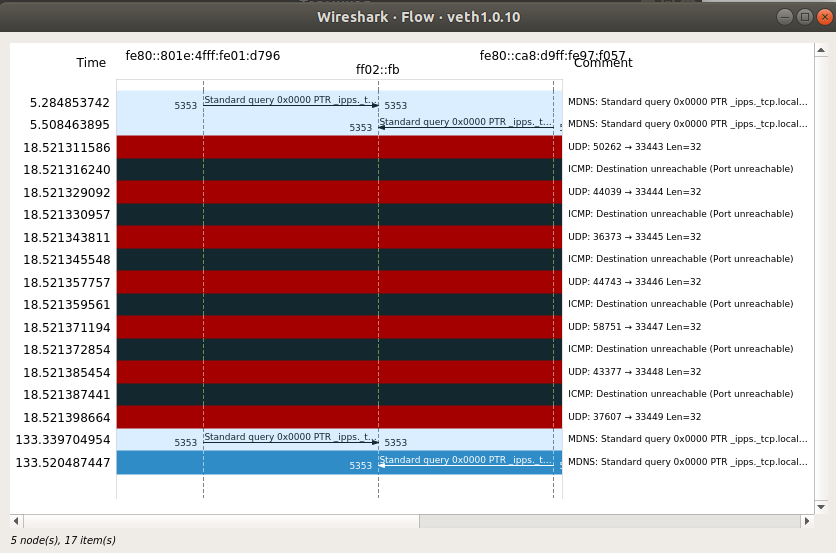


3) Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.

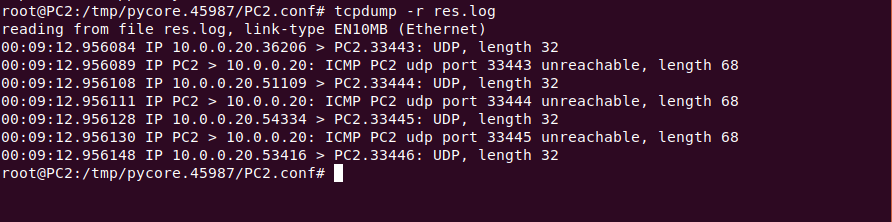
Передаю пакеты с PC2 на PC1. Отслеживаю их в Wireshark

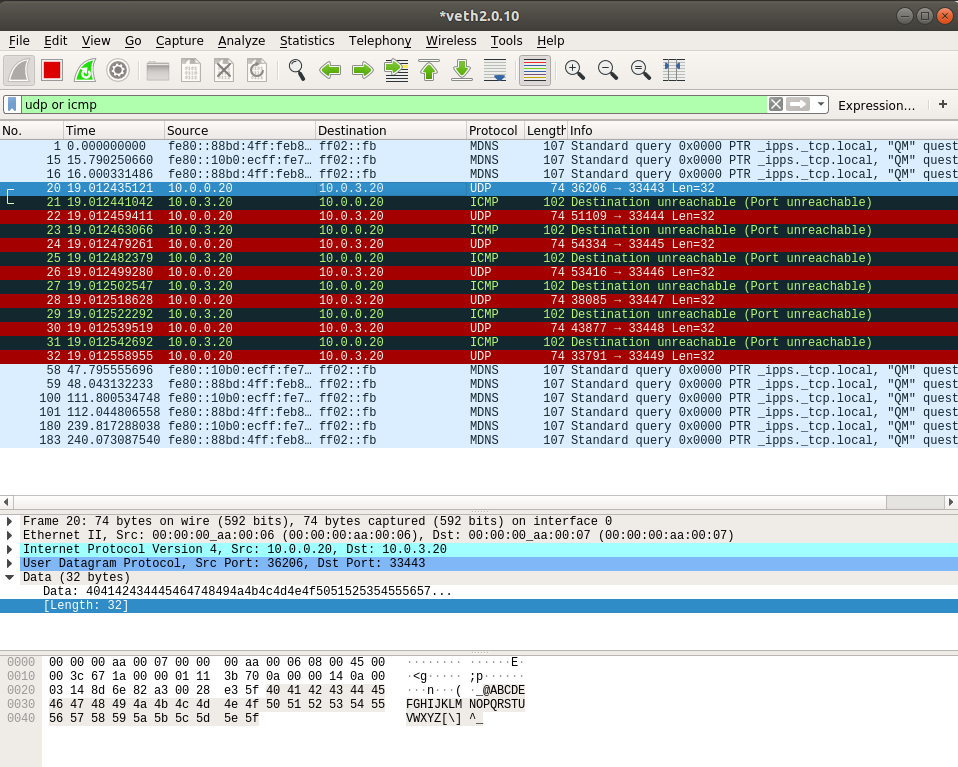


Получаю диаграмму:



4) Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.





В Wireshark отображается более детальная информация о пересылаемых пакетах